The Federal Information Security Management Act of 2002

By James E. Collins

What is FISMA?

The Federal Information Security Management Act of 2002 (FISMA) is contained within the E-Government Act of 2002 (Public Law 107-347), replacing the Government Information Security Reform Act (GISRA). FISMA, effective throughout the federal government, places requirements on government agencies and components, with the goal of improving the security of federal information and information systems.

What is the purpose of FISMA?

The purpose of FISMA is as follows:

√ Provide a framework for enhancing the effectiveness of information security in the federal government. This means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to ensure integrity, confidentiality and availability.

√ Provide effective government-wide management of risks to information security.

√ Provide for the development and maintenance of minimum controls required for protecting federal information and information systems.

√ Provide a mechanism for effective oversight of federal agency information security programs.

What does FISMA require?

FISMA requires the head of each federal agency to provide information security protections commensurate with the risk and magnitude of the harm that may result from unauthorized access, use, disclosure, disruption, modification or destruction of its information and information systems. The protection should apply not only within the agency, but also within contractor or other organizations working on behalf of the agency.

FISMA requires that the agency head delegate to the agency Chief Information Officer (CIO) the authority to ensure compliance with the legislation. Further, the CIO must designate a senior agency information security officer whose primary duty is to carry out the CIO's responsibilities for information security. This information security officer must possess commensurate professional qualifications, training and experience, and head an office with sufficient resources to carry out information security responsibilities. In the case of the Department of the Navy (DON), "agency head" refers to both the Secretary of Defense and the Secretary of the Navy. Within the Department of the Navy, Dave Wennergren, DON CIO, designated Rob Carey, Deputy CIO for Policy and Integration, as the senior DON information security officer.

The FISMA law requires that the CIO carry out the following responsibilities:

• Develop and maintain an agency-wide information assurance (IA) program complete with policies, procedures and control techniques to address information security requirements, including FISMA.

• Ensure that required training is conducted including annual information security training and Internet security training.

• Ensure oversight of personnel with significant responsibilities for information security.

• Assist senior agency officials concerning their awareness and responsibilities for information and information system security.

The law also requires the agency head, in this case the Secretary of the Navy, to:

• Ensure the agency has a sufficient number of trained personnel to ensure agency-wide IA.

• Require annual reports from the CIO regarding the effectiveness of agency IA programs and progress on any required remedial actions.

Specifically, FISMA requires each federal agency to develop, document and implement an agency-wide information security program, which includes the following:

• Periodic risk assessments.

• Risk assessment policies and procedures that cost-effectively reduce the risk to an acceptable level, ensure that information security is addressed throughout the life cycle of each agency information system and ensure compliance with FISMA.

• Subordinate plans for networks, facilities and groups of systems as appropriate.

• Security awareness training for agency personnel, including contractors and system users.

• Periodic (at least annual) testing and evaluation of the effectiveness of information security policies, procedures and practices.

• Processes for planning, implementing, evaluating and documenting remedial action to address deficiencies in agency information security policies, procedures and practices.

• Procedures for detecting, reporting and responding to security incidents.

• Plans and procedures to ensure continuity of operations for information systems that support agency operations and assets.

FISMA requires each federal agency to report to Congress annually by the first of March. The report must address the adequacy and effectiveness of information security policies, procedures and practices. In addition to the annual report, FISMA requires each agency to conduct an annual independent evaluation of the IA program and practices to determine their effectiveness.

The FISMA legislation assigns to the Department of Defense (DoD) the authority to develop and oversee the implementation of IA policies, principles, standards and guidelines. The legislation also requires DoD components to identify and provide information security protective measures commensurate with the risk and magnitude of the harm possibly resulting from unauthorized acts.

What is the impact of FISMA on the DON?

Many of the aspects of FISMA are already in place, such as IA training, incident reporting and testing. DON CIO is preparing policies and plans to carry out the law's requirements, including the basic Secretary of the Navy policy on information assurance, Secretary of the Navy Instruction (SECNAVINST) 5239.3.

The DON CIO has submitted the required annual reports for three years, first for GISRA and this year for FISMA. In practice, DON CIO coordinates with the Navy and the Marine Corps and submits an annual DON FISMA input to DoD. DoD then submits a composite Defense-wide report to the Office of Management and Budget (OMB), which in turn submits the report to Congress as required by the legislation. The relevant Inspectors General and audit services conduct the required annual evaluations, which include site visits, testing and assessments.

FISMA, effective throughout the federal government, places requirements on government agencies and components, with the goal of improving the security of federal information and information systems.

In summary, the overarching goal of the Department of the Navy is to secure the Department's information assets, balancing the need for security with the primary objective of meeting operational requirements. By doing that, we are well along the way to compliance with FISMA.

Mr. Collins is a retired Navy captain providing support to the DON CIO IA Team.

The DON eGov Awards Fall 2003

The Department of the Navy Chief Information Officer (DON CIO) is pleased to announce the winners of the Fall 2003 DON eGov Awards. These awards honor project teams that have successfully reengineered/transformed key DON business and warfighting processes to reduce costs, improve mission performance, and support the effective exchange and sharing of information.

The following teams are honored for their successful initiatives, which are leading the way toward the eGovernment transformation of the DON:

- Marine Corps Systems Command, HQMC, Manpower & Reserve Affairs & DFAS - Technical Services Organization for Total Force Administration System (TFAS)
- Commander, Naval Reserve Force, DFAS - Technical Services Organization & SPAWAR Information Technology Center for Naval Reserve Order Writing System (NROWS)
- NAVAIR Aircraft Wiring Support Equipment Commodity & eBusiness Operations Office for Just-in-Time Wiring Information System (JITWIS) eSuite
- ASRLW NAVAIR Team & eBusiness Operations Office for Aircraft Shot and Recovery Log - Web (ASRLW)
- ePMS NAVSEA Team & eBusiness Operations Office for Electronic Planned Maintenance System (ePMS)
- USS Dwight D. Eisenhower & eBusiness Operations Office for Refueling and Complex Overhaul Integrated Maintenance Package
- Task Force Web for Building the Web Enabled Navy (WEN)
- NETC Business Office for NETC Military Awards Processing System (NMAPS)

The eGov awards were presented at the Fall 2003 Naval IT Summit held in Arlington, VA. This first DON IT Summit brought together the DON CIO, DON Deputy CIO (Marine Corps), DON Deputy CIO (Navy) and command information officers from Echelon II and major Marine Corps subordinate commands in a forum to build the Navy-Marine Corps team and advance our strategy for continual transformation.

Look for more information about the IT Summit and the eGov Awards in the next issue of CHIPS.